Requirements Engineering

(Summer 2019)

Prof. Nan Niu (nan.niu@uc.edu)

http://homepages.uc.edu/~niunn/courses

Today's Menu

Last Seminar:
"req.s", "why", & "RE"

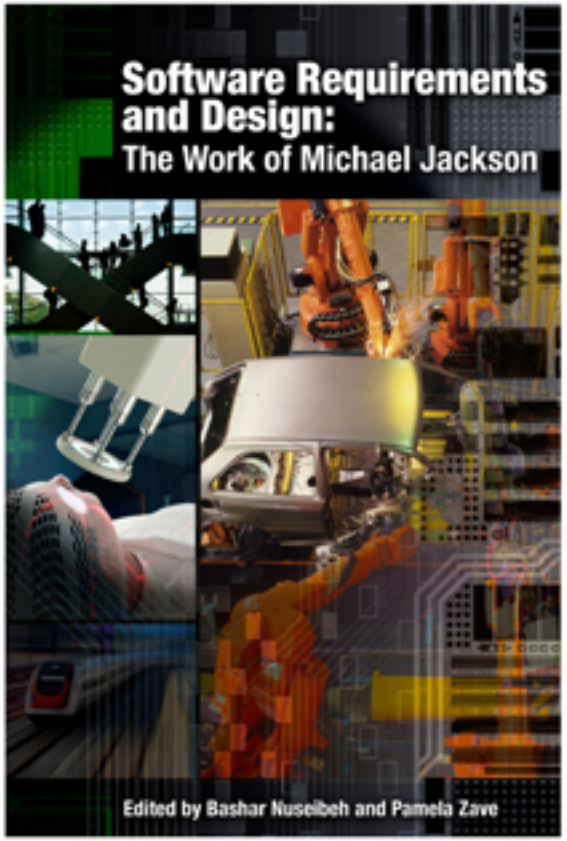
This Seminar:
Meaning of Req.s

Next Seminar:
Req.s Elicitation
Goal Modeling (ASN1)

The Meaning of Requirements

Software Requirements and Design: A Tribute to Michael Jackson

ICSE 2009 VANCOUVER



Michael Jackson (not the singer)

$$\mathcal{E}, S \vdash R$$

Source: *Jackson's Website, & ICSE'09 Website*

The *req.s* concerned in Jackson's paper

- The computer must not weigh more than 0.25 Kg.
- The system must be completed by 1st January 1998.
- The programs must be written in Ada.
- The system specification must be formally accepted by the steering committee.
- The operator interface must be easy to learn.
- The system must produce a monthly report of outstanding debts.
- If passenger in the lift presses the *open-doors* button while the lift is stationary at a floor, the doors should begin to open within 0.5 secs.

→Functional requirements

↳Real-time response

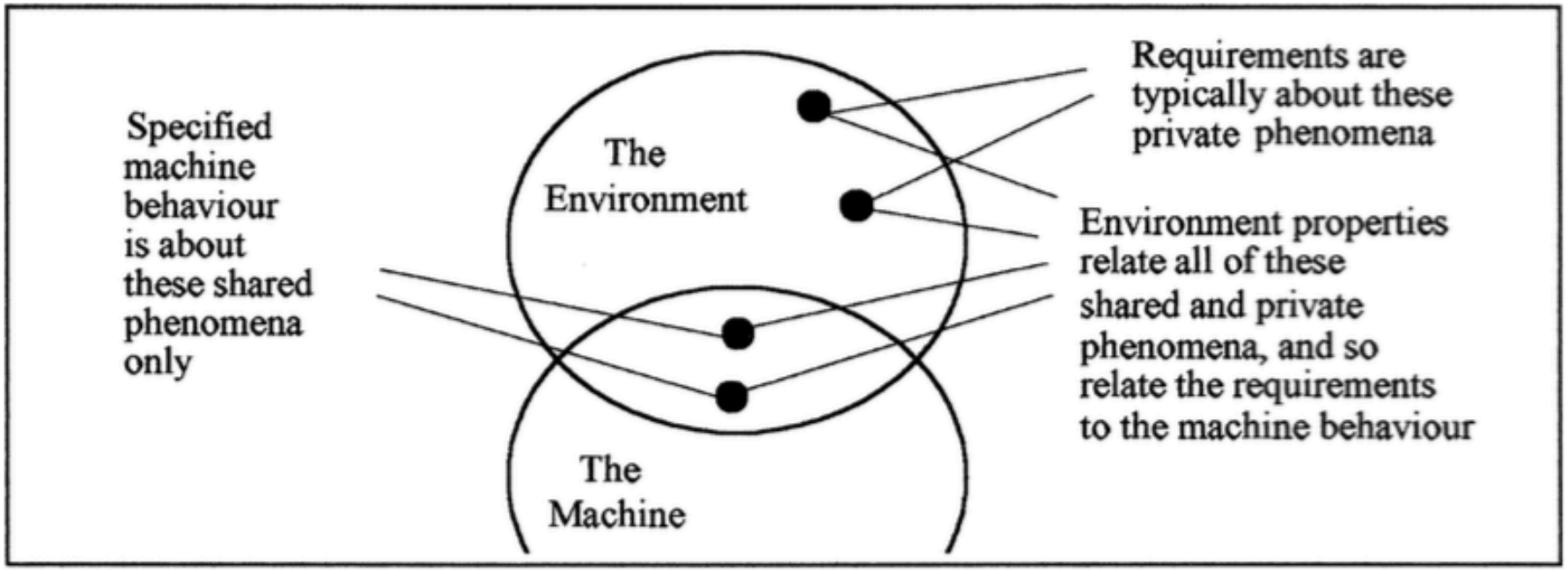
↳Those properties (of operational safety that) can be *precisely* stated in terms of system behavior

Requirements are in environment

- Environment = the part of the world
  - into which the machine will be installed
  - with which the machine will interact
  - in which the effects of the machine will be observed and evaluated
- Machine = software-to-be
  - with which programmers do programming
  - sth. that we transform a general-purpose computer into in order to satisfy stakeholder needs & desires

We want to do programing/transformation without further environment knowledge. ← What RE is for.

Understanding R, Ɛ, S



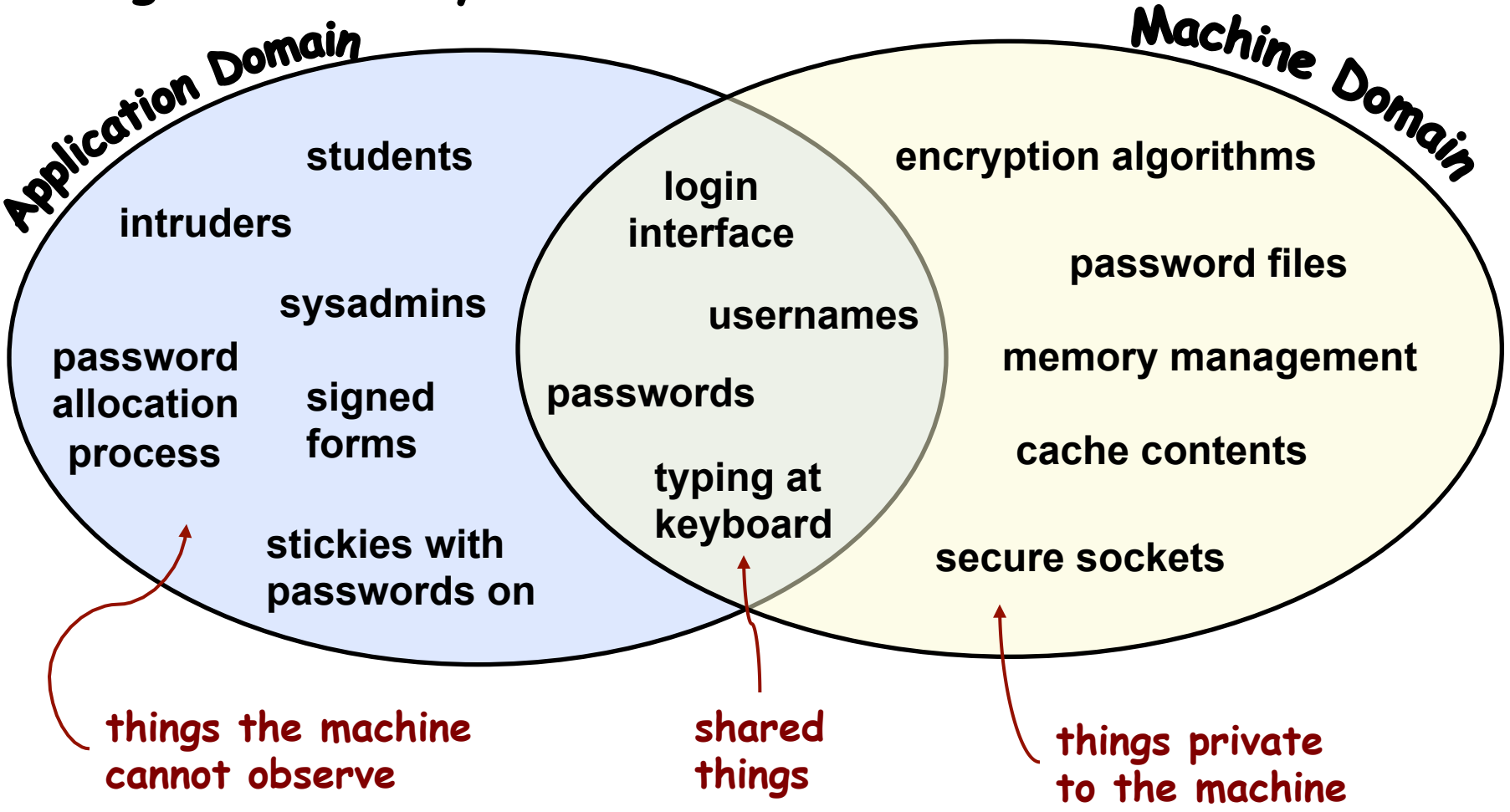
R: requirements (optative/desired)

Ɛ: environmental assertions (indicative/given)

S: specifications (optative/desired)

Software is a science of description

→ E.g. "allow only authorized access to lab machines"



To be more specific

- Requirement R:
  - "The lab machine shall be accessible by only authorized personnel"
- Domain Properties E:
  - Authorized personnel have usernames
  - Authorized personnel have passwords
  - Passwords are never shared with non-authorized personnel
- Specification S:
  - Access to the lab machine shall be granted only after the user types an authorized "username, password" pair
- S + E entail R

In-Class Exercise #1: Group

→Form your group

→Instantiate R, Ɛ, S for the elevator system such that your instantiated R, Ɛ, S satisfy "Ɛ,S |- R".

My Answer to Exercise #1

→R: "attend a class at a different floor"

→Requirement is in the OPTATIVE mood, expressing a wish

→Requirement can (and SHOULD) be stated entirely without reference to the machine

- Private phenomena of the environment
- Requirements are located in the environment

→The GOAL (needs & desires) of stakeholders

Environmental Assertions

→ R: "attend a class at a different floor"

→ E is in the INDICATIVE mood, expressing what is claimed to be a known truth

→ Instances of E: knowing …

- "different floor of the SAME building"
- "LOCATION of the elevator inside the building"
- "DIRECTION ('up' or 'down') to go"
- …

Finally: "Ɛ,S |- R"

→ R: "attend a class at a different floor"

→ Ɛ: …, "press the right button", …

→ S: "button ➔ sensor ➔ controller ➔ move"

→ Specification

- Optative
- Shared phenomena of environment and machine
- A nexus of constraints and causal chains

The meaning of requirements: "Ɛ,S |- R"

RE, in its simplest form, shall (1) elicit R, and (2) derive S such that "Ɛ,S |- R"

Ɛ should act as a sufficient faithful approximation to the informal environment.

We want to do programming without further environment knowledge. ← What RE is for.

How to build a narrow bridge?

→Designation of ground term

- associates a formal ground term, such as a predicate, with the denoted phenomena, such as an event or entity class or a relationship over events or entities

$$\text{Mother}(x, y) \cong x \text{ is the mother of } y.$$

Left-hand side: formal term

informal recognition rule by which the designated phenomena may be unambiguously recognized

Right-hand side: non-formal world (physical, social, …)

RE Silver Jubilee Special Session

$$\text{Mother}(x, y) \cong x \text{ is the mother of } y.$$

Left-hand side: formal term

informal recognition rule by which the designated phenomena may be unambiguously recognized

Right-hand side: non-formal world (physical, social, …)

Silver Jubilee

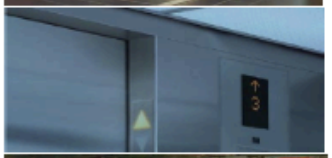
Michael Anthony Jackson:
The Right-Hand Side Problem: Research Topics in RE. 474-475

Right-hand side problem

→relationship of formal models to physical reality

Radiation therapy

Passenger lift



Rotterdam barrier

Car parking

Flight control

Cruise control

Software-intensive systems

→ are engineered to fulfill the ***requirements*** that are located in the environment

Industrial press

Vending machine

Medical Records

Lending Library

Besides "designation", "definition" can help build a narrow bridge

→ Definition to clarify phenomena

- Suppose the following *designations* have already been made:

$$\begin{aligned}
\text{Plane}(p) &\cong p \text{ is a plane,} \\
\text{Land}(e,p,t) &\cong \text{In event } e \text{ the plane } p \text{ lands at time } t, \\
\text{TakeOff}(e,p,t) &\cong \text{In event } e \text{ the plane } p \text{ takes off at time } t.
\end{aligned}$$

- We can *define* a "flight" as it applies to air travel, and more importantly, as it is *useful* in talking about airline operations
  - e.g., a plane on the ground is not considered "flight DL 189"

Is this "flight" definition good?

Given

$$\text{Plane}(p) \cong p \text{ is a plane,}$$

$$\text{Land}(e, p, t) \cong \text{In event } e \text{ the plane } p \text{ lands at time } t,$$

$$\text{TakeOff}(e, p, t) \cong \text{In event } e \text{ the plane } p \text{ takes off at time } t.$$

Define

$$\text{flight} \stackrel{\text{def}}{=} \big(p, e, f, t1, t2 \mid \text{Plane}(p) \wedge \text{TakeOff}(e, p, t1) \wedge \text{Land}(f, p, t2)\big).$$

A better definition

$$\stackrel{\text{def}}{=} (p, e, f, t1, t2 \mid \text{Plane}(p) \wedge \text{TakeOff}(e, p, t1) \wedge \text{Land}(f, p, t2) \wedge t1 < t2 \wedge \neg (\exists g, t3 \bullet (\text{Land}(g, p, t3) \wedge t1 < t3 < t2))).$$

What's "good"?

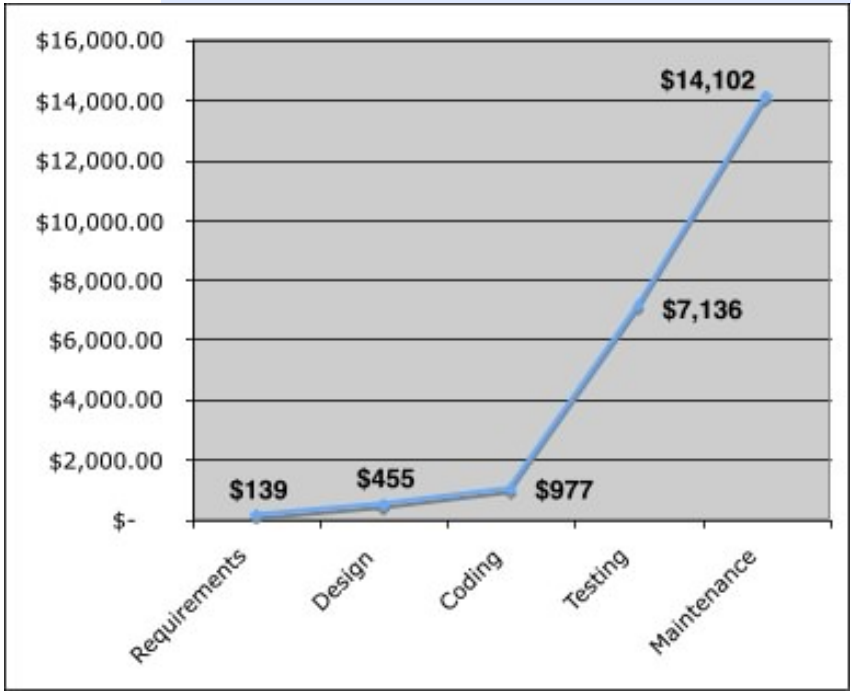
Complete

Consistent

Unambiguous

...

Here's "why"?



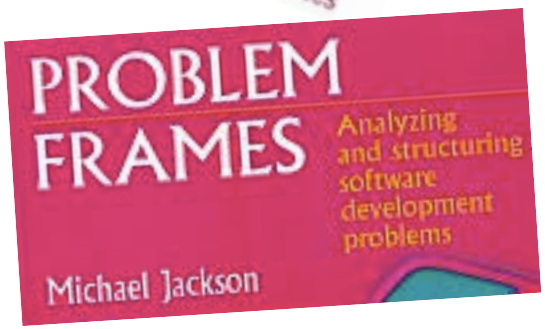
Jackson's own conclusion

> Requirements engineering is not a branch of pure mathematics or logic: the meaning and applicability of an environment description depends crucially on its reliable interpretation in the environment. In requirements engineering we may not postpone interpretation until description is complete: without its interpretation a description at any level is literally meaningless.

$$\mathcal{E}, S \vdash \mathcal{R}$$

Beauty in Software Engineering

Jon G. Hall and Lucia Rapanotti
The Open University



Any Questions?

Functional vs. Nonfunctional

- Functional requirements describe **WHAT** the software does
- Nonfunctional requirements (NFRs) describe **HOW WELL** the software does it
- Implications: Elicitation, modeling, analysis, realization, validation, evolution … of NFRs are different from those of functional requirements

It's not just about moving…

Comfort

Safety

Usability

Accessibility

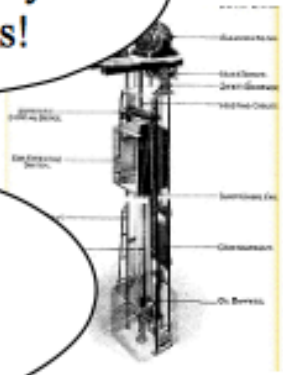
descriptions used in RE that are *not refutable* are vague & should only be treated as *rough sketches*

System Complies with All Safety Regulations!

Easy to Use Floor-to-Floor Transport!

Lift Comes when I Request and Goes to the Floor I Choose!

Safe Operation by Firefighters!



Don't Try My Patience!

Graceful Service Degradation on Minor Failures!

Perfect Lift Service Sells Apartments & Offices!

I can Specify VaryingRegimes!

Efficiency Means Fewer Lifts, More Rentable Space!

Don't Damage the Equipment by Misuse!

Easy Operation in Maintenance!

No Lower Classes on my Floor!

Easy Quarterly Inspections!

Summary

- → Meaning of requirements
  - ↳ Requirements are located in the *environment*, in which the effects of the machine will be observed and evaluated
  - ↳ Specification forms a bridge between RE and SW Eng

    $\mathcal{E}, S \vdash R$
  - ↳ Making a *narrow* bridge involves
    - ➢ Designation, definition, assertion
    - ➢ Right-hand side problem ➔ research topics in RE
- → Desiderata of the *descriptions* used in RE
  - ↳ Complete, consistent, unambiguous … refutable …
- → Next
  - ↳ Requirements elicitation
  - ↳ Goal modeling (ASN1)

Meaning of Requirements